AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

(1) INFORMATION ASSOCIATED WITH THE GOOGLE, LLC. ACCOUNTS UTILIZING THE FOLLOWING IDENTIFIERS:
A. [redacted]GMAIL.COM; PHONE NUMBER 310-[redacted]
B. [redacted]@GMAIL.COM; PHONE NUMBER: 310-[redacted]
C. [redacted]@GMAIL.COM; PHONE NUMBER: 845[redacted]
THAT ARE STORED AT THE PREMISES CONTROLLED BY GOOGLE, LLC.

UNDER SEAL

Case No. 2:23sw: 11

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):* **See Attachment A-1.**
located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*
See Attachment B-1.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description*
18 U.S.C. §2251(a)(1)	Production of Visual Depictions of Minors Engaging in Sexually Explicit Conduct
18 U.S.C. §2252(a)(1)	Transportation of Visual Depictions of Minors Engaging in Sexually Explicit Conduct
18 U.S.C. §2252(a)(2)	Receipt or Distribution of Minors Engaging in Sexually Explicit Conduct
18 U.S.C. §2252(a)(3)(B)	Sale of Visual Depictions of Minors Engaging in Sexually Explicit Conduct
18 U.S.C. §2252(a)(4)(B)	Possession of Visual Depictions of Minors Engaging in Sexually Explicit Conduct
18 U.S.C. §2422(b)	Coercion and Enticement of a Minor

The application is based on these facts: **See Affidavit.**

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S .C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

Date: January , 2023

Kristen S. Taylor
Assistant United States Attorney

Applicant's signature

NCIS Special Agent Stephen Barbour
Printed name and title

Sworn to before me and signed in my presence.

Date: Jan. 26, 2023

Judge's signature

City and state: Norfolk, Virginia

ROBERT J. KRASK
UNITED STATES MAGISTRATE JUDGE
Printed name and title

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information, wherever stored, associated with

a) [redacted]l@gmail.com; Phone Number: 310-[redacted]
b) [redacted]@gmail.com; Phone Number: 310[redacted]
c) [redacted]@gmail.com; Phone Number: Phone Number: 845-[redacted]

wherever located, which is or was stored at premises owned, maintained, controlled, or operated by Google, LLC., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, including the information preserved pursuant to an October 28, 2022, request by the United States Attorney's Office.

ATTACHMENT B-1

Particular Things to Be Seized

I. Information to be disclosed by Google, LLC. (the "Provider")

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held, or maintained inside or outside the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1, for the time period of January 1, 2021 to the present:

a. Account Information - User name, primary email address, secondary email addresses, connected applications and sites, and account activity including account sign in locations, browser information, platform information, account status, and internet protocol (IP) addresses;
b. Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) of all associated devices linked to the Google accounts of the target device;
c. Evidence of user attribution - accounts, email accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).
d. Gmail – The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;
e. Contacts – Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
f. Calendar – Any records pertaining to the user's calendar(s), including Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
g. Messaging – The contents of all tex, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

h. Google Drive and Keep – The contents of all records associated with the account in Google drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including files, folders, media, notes, and note titles, lists, applications, and other data uploaded, created, stored, or shared with the account, including drafts and deleted records; third party application data and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service, or third party application associated with each record; and all associated logs, including access logs and IP addresses of each record;

i. Photos – The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

j. Maps – All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, time stamps, and change history;

k. Location History – All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date, and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

l. Google Pay – All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records or purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP addresses, time stamps, location data, and change history;

m. Chrome and My Activity – All internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, Google Home, including search queries and clocks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts; subscriptions; and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

n. Google Voice – All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages;

voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history;

o. A list of linked accounts based upon IP address and session cookie;
p. The types of services utilized;
q. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and
r. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 2251(a), 2422(b), 2252(a)(1), (a)(2), (a)(3), and (a)(4) involving Jameson Ross WEED and others, including for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

a) Evidence of criminal activity.
b) Communication between KNOWN and UNKNOWN SUBJECT(S) involved in the crimes under investigation.
c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
d) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s) with whom he communicated;
f) The identity of the person(s) who communicated with the user ID about matters relating to the crime under investigation, including records that help reveal their whereabouts.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e., communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team will then provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. This

investigation is presently covert, and the government believes that the subject of the search is not aware of this warrant.

III. Disclosure by the Provider

Notwithstanding 18 U.S.C. § 2251 *et seq*. or similar statute or code, Google, LLC. shall disclose responsive data, if any, within fourteen days of service of the warrant, by sending it to Naval Criminal Investigative Service (NCIS) Special Agent Stephen Barbour (Stephen.barbour@ncis.navy.mil) located at (1329 Bellinger Blvd., Building U-40 Norfolk, VA 23511) using the U.S. Postal Service or another courier service or by electronic means.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

IN THE MATTER OF THE SEARCH OF:		UNDER SEAL
(1) INFORMATION ASSOCIATED WITH THE GOOGLE, LLC. ACCOUNTS UTILIZING THE FOLLOWING IDENTIFIERS: A [redacted]@GMAIL.COM; PHONE NUMBER [redacted]2071 B [redacted]@GMAIL.COM; PHONE NUMBER: [redacted]2071 C. [redacted]@GMAIL.COM; PHONE NUMBER [redacted]-3538 THAT ARE STORED AT THE PREMISES CONTROLLED BY GOOGLE, LLC.	)	Case No. 2:23sw 11
(2) INFORMATION ASSOCIATED WITH THE SNAPCHAT ACCOUNTS: A. USERNAME: JAYRW1701 B. USERNAME: BABYGIRL_LUNA44 THAT ARE STORED AT THE PREMISES CONTROLLED BY SNAP, INC.	)	Case No. 2:23sw 12
(3) INFORMATION ASSOCIATED WITH THE INSTAGRAM ACCOUNT UTILIZING THE FOLLOWING IDENTIFIERS: A. USERNAME: JAMESRWEED1701; EMAIL: [redacted]@GMAIL.COM; PASSWORD: JAYMAN1701 THAT IS STORED AT THE PREMISES CONTROLLED BY META PLATFORMS, INC.	)	Case No. 2:23sw 13

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Stephen Barbour, being first duly sworn state:

INTRODUCTION AND AGENT BACKGROUND

1. I am employed by the Naval Criminal Investigative Service (NCIS). I have been employed as a Special Agent for over thirteen years. My current assignment is at the NCIS Resident Agency in Norfolk, Virginia, and I am tasked with investigating criminal offenses, including certain activities relating to material constituting or containing child pornography. I have

been trained in various aspects pertaining to the enforcement of federal laws, the law of the Uniform Code of Military Justice (UCMJ), and criminal offenses committed by certain members of the U.S. Armed Forces. I have a Bachelor of Science degree in Psychology from James Madison University, Harrisonburg, Virginia. I am a graduate of the Criminal Investigator Training Program and the Special Agent Basic Training Program at the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia. Additionally, I am certified to conduct peer-to-peer investigations through the Ohio Peace Officer Training Commission, and I am certified by the Internet Crimes Against Children (ICAC) training and technical assistance program to conduct undercover child exploitation investigations. I am also a certified Child Forensic Interviewer (CFI). Prior to my employment with NCIS, I was employed as a sworn police officer with the Virginia Beach Police Department for six years. Additionally, I served on active duty in the United States Marine Corps for four years and received an honorable discharge at the end of my service at the rank of Sergeant. I have been conducting federal, state, and military criminal investigations for more than nineteen years to include numerous cases involving sexual assault, child molestation, crimes against children, child pornography, and various other criminal enterprises. I have become familiar with the manner and means by which criminals commit and conceal criminal offenses, and the places in which evidence of such crimes can be located. I have prepared affidavits in support of and participated in the execution of numerous search warrants and command authorizations relating to violations of federal, state, and military laws and have received training regarding the collection and preservation of digital evidence on electronic devices.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The information set forth in this affidavit is known to me as a result of an investigation personally conducted by me and other law enforcement agents. Thus, the statements in this affidavit are based in part on information provided by other investigators employed by federal or state governments.

4. This affidavit is made, in part, in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, LLC., Snap Inc. and Meta Platforms, Inc., (the "Providers") to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the accounts, including the contents of communications. The information to be searched and seized is described in the following paragraphs and in Attachments A-1, A-2, and A-3, further described in Attachments B-1, B-2, and B-3.

5. This affidavit is being submitted in support of an application for a search warrant for the information and content associated with the SUBJECT ACCOUNTS, specifically described as:

A. Google accounts associated with the following identifiers:

a. [redacted]@gmail.com; Phone Number [redacted]2071
b. [redacted]n@gmail.com; Phone Number [redacted]2071
c. [redacted]@gmail.com; Phone Number: [redacted]-3538

from January 1, 2021 to present, which are stored at premises owned, maintained, controlled, or operated by Google, LLC., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, as described in Attachment A-1.

B. Snapchat accounts:

a. Username: jayrw1701
b. Username: babygirl_luna44

from January 1, 2021 to present, which are stored at premises owned, maintained, controlled, or operated by Snap Inc., a company headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405, as described in Attachment A-2.

C. Instagram account associated with the following identifiers:

a. Username: Jamesrweed1701; Email: [redacted]l@gmail.com; Password: Jayman1701

From January 1, 2021 to present, which are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1601 Willow Road, Menlo Park, CA 94025, as described in Attachment A-3.

6. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251(a) (production of visual depictions of minors engaging in sexually explicit conduct); 18 U.S.C. § 2422(b) (coercion and enticement of a minor); 18 U.S.C. § 2252(a)(1) (transportation of visual depictions of minors engaging in sexually explicit conduct); 18 U.S.C. § 2252(a)(2) (receipt or distribution of visual depictions of minors engaging in sexually explicit conduct); 18 U.S.C. § 2252(a)(3)(B) (sale of visual depictions of minors engaging in sexually explicit conduct); and 18 U.S.C. § 2252(a)(4) (possession of visual depictions of minors engaging in sexually explicit conduct) (the "Target Offenses") have been committed by Jameson Ross WEED ("WEED"). There is also probable cause to search the information described in Attachments A-1, A-2, and A-3 for evidence of these crimes, as further described in Attachments B-1, B-2, and B-3.

JURISIDICTION

7. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the court is "a district court of the United States… that has jurisdiction over

the offense being investigated." 18 U.S.C § 2711(3)(A)(i). This investigation involves an offense within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated below.

PERTINENT FEDERAL CRIMINAL STATUTES

8. *Title 18, United States Code § 2251(a)* makes it a crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

9. *Title 18, United States Code, § 2422(b)* makes it a crime for a person, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense.

10. *Title 18, United States Code, § 2252(a)(1)* makes it a crime to knowingly transport or ship using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and such visual depiction is of such conduct.

11. *Title 18, United States Code, § 2252(a)(2)* makes it a crime to knowingly receive or distribute, using any means or facility of interstate or foreign commerce or that has been mailed, shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed, shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, any visual depiction of minors engaging in sexually explicit conduct.

12. *Title 18, United States Code, § 2252(a)(3(B)* makes it a crime to knowingly sell or possess with intent to sell any visual depiction that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or has been shipped or transported in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported using any means or facility of interstate or foreign commerce, including by computer, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and such visual depiction is of such conduct.

13. *Title 18, United States Code, § 2252(a)(4)(B)* makes it a crime to knowingly possess or access with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in

or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer.

LEGAL AUTHORITY

14. The legal authority for this search warrant application regarding electronic mail accounts is derived from 18 U.S.C. §§ 2701-2711, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides in relevant part as follows:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

18 U.S.C. § 2703(b) provides in relevant part as follows:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.
>
> (2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –
>
> (A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
>
> (B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

15. The government may also obtain records relating to email communications, such as subscriber identifying information, by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A).

16. 18 U.S.C. § 2703(c)(1)(A), provides, in part, that the Government may also obtain non-content records and other information pertaining to a customer or subscriber of an electronic communication service or remote computing service by means of search warrant.

17. 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

DEFINITIONS

18. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

19. "Child Erotica" as used herein, refers to materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions. Such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

20. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device," and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

21. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

22. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

23. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

24. "Electronic Communication Service" refers to any service, which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

25. "Electronic Communications System" means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

26. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

27. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

28. "Internet Protocol Address" (IP Address), as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP Addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP Addresses might also be "static," if an ISP assigns a user's computer a particular IP Address that is used each time the computer accesses the Internet.

29. "Minor" and "sexually explicit conduct" are defined in 18 U.S.C. §§ 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

a. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
b. Bestiality;
c. Masturbation;
d. Sadistic or masochistic abuse; or
e. Lascivious exhibition of the genitals or pubic area of any person.

30. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

31. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." 18 U.S.C. § 2711.

32. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

33. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting

facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

BACKGROUND CONCERNING GOOGLE[1]

34. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

35. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

1 The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

36. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

37. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

38. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

39. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

40. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

41. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

42. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile

phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

43. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

44. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive.

45. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

46. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from

one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely unless the user deletes it.

47. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen

months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

48. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

49. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

50. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home

voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

51. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

52. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

53. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

54. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the IP Addresses used to register the account and accept Google's terms of service, as well as the IP Addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP Address, IP Address information can help to identify which computers or other devices were used to access the Google Account.

55. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

56. According to Google's Privacy & Terms website https://www.google.com/policies/technologies/cookies) the company sends a small piece of text (known as a "cookie"') to the user's Internet browser for a variety of purposes. Cookies allow the websites visited, such as Google.com or Gmail.com, to recognize the electronic device that is accessing that website.

Google's cookies record: (a) all of the Google accounts accessed by a particular electronic device using the same web browser; (b) information about those visits; and (c) the user's preferences and other settings. When that device returns to the website later, Google can then tailor the user's online experience accordingly. Using these cookies, Google is able to establish a relationship between Google accounts that are used by the same individual.

BACKGROUND INFORMATION REGARDING SNAPCHAT

57. Snapchat is one of the most popular applications for sending and receiving "self-destructing" messages, pictures, and videos. Referred to as "snaps", the company processes approximately 700 million of them every day on Apple's iOS and Google's Android operating systems. Snapchat users access the application frequently. According to marketing material provided by the company, the average Snapchat user checks their account 14 times a day.

59. A "snap" is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed, it is deleted from the company's system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaved the Chat screen, messages viewed by both the sender and the receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device.

60. Snapchat asks users to provide basic contact and personal identifying information to include date of birth. When a user creates an account, they make a unique Snapchat username. This is the name visible to other Snapchat users. An email address is required to register a Snapchat

account and a new user must also provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code which must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.

BACKGROUND CONCERNING INSTAGRAM2

61. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

62. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

63. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create

2 The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Privacy Policy," https://privacycenter.instagram.com/policy/; "Information for Law Enforcement," https://help.instagram.com/494561080557017; and "Help Center," https://help.instagram.com.

and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

64. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

65. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

66. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

67. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

68. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

69. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

70. Users can interact with posts by liking them, adding, or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on several factors, including privacy settings and which users were tagged or mentioned.

71. An Instagram "story" is like a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

72. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

73. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

74. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

75. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

76. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

77. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

78. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user because of the communications.

79. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

PROBABLE CAUSE

80. On June 13, 2022, NCIS Resident Unit, Naval Medical Center Portsmouth (NMCP) received a request from New York State Police (NYSP) Senior Investigator Timothy Jordan for investigative assistance regarding WEED's alleged involvement in various criminal offenses involving a minor victim, S.C. On or about June 13, 2022, S.C.'s parents were notified by NYSP that an unidentified party disclosed information to school administrators suggesting that S.C. (16 years old at the time) was involved in a relationship with an older man. S.C.'s parents subsequently discovered evidence of this relationship among S.C.'s belongings at their residence, including a Choice Hotels key card, which S.C.'s parents turned over to NYSP.

81. On June 13, 2022, NYSP investigators interviewed S.C. and her parents. S.C. voluntarily surrendered her cell phone and computer as evidence and provided a list of usernames and passwords associated with her social media accounts. Specifically, S.C. provided her Snapchat Username: "babygirl_luna44," and the password to the "other Instagram" (the Instagram account WEED allegedly used to advertise her sexually explicit photos and videos): "Jayman1701."

82. S.C. stated that on or about January 28, 2022, S.C. met WEED on a website called "Fetlife.com." "Fetlife.com" is a social networking website for the BDSM ("bondage and discipline, dominance and submission, sadochism and masochism") fetish, and "kinky" community. WEED direct messaged S.C. on the website and they exchanged contact information. WEED and S.C. maintained an online relationship using multiple electronic platforms, including, Snapchat, Instagram, and Google.

83. S.C. advertised that she was 18 years old on the "Fetlife.com" website. After WEED began talking to S.C. using other electronic mediums, including Snapchat, S.C. was not initially forthcoming about her actual age. When asked by WEED for some form of proof that she

was 18, S.C. balked, and advised WEED that she had no physical proof. S.C. later asked WEED how he would react if she was not 18. WEED responded that his reaction would depend on how much younger she was. WEED's response suggested that WEED was familiar with the age of legal consent in New York – S.C.'s place of residence – and federal laws regarding child pornography.

84. A little over a week into WEED's online "relationship" with S.C., on or about February 8, 2022, S.C. discussed family issues with WEED. S.C. told WEED that she planned to get out of her family home as soon as she graduates and then stated, "[t]hey can't make me stay. Im 16. My own father ran away/moved out at 16." WEED responded, "Please don't run away, even without them. It truly doesn't solve anything. . . [followed by] True True, I just don't want to see you go through all of that." S.C. stated that she advised WEED that she was 16 years old shortly after they connected. The chats confirm that by at least on or about February 8, 2022, WEED was advised by S.C. that she was 16 years old. In fact, the substance of the conversation on February 8, 2022 suggests WEED was aware of S.C.'s actual age before then. WEED was 24 years old at the time. WEED also referred to S.C.'s "underage pussy" and his "experienced cock" multiple times during their sexually explicit Snapchat conversations.

85. S.C. stated that she and WEED exchanged explicit photos and videos using various platforms, including Snapchat. S.C. further stated that she was cautious not to show her face in any of the photos or videos she sent to WEED until approximately one month into their "relationship." According to S.C., WEED edited some of S.C.'s explicit photos and videos and then posted them online. Furthermore, S.C. stated that WEED sold some of S.C.'s photos and videos using Instagram. S.C. received some of the proceeds from the sales of her photos and videos via a Cash App account WEED created for this purpose. S.C. provided more detail regarding this

arrangement in a subsequent interview conducted by your affiant as discussed in more detail below.

86. Also, during her June 13, 2022 interview, S.C. described an in-person encounter with WEED that took place on or about March 26-27, 2022. S.C. stated that WEED traveled from Virginia to New York (NY) and picked S.C. up from her residence located in Hyde Park, NY. WEED and S.C. then traveled to the Crossroads Hotel in Newburgh, NY. According to S.C., WEED furnished S.C. with CBD edibles, a vape, and alcohol. S.C. and WEED then engaged in unprotected consensual oral sex and vaginal intercourse. Some of the sexual activity that took place between WEED and S.C. was recorded. Specifically, S.C. believes S.C. recorded herself having sex with WEED and sent WEED the video. According to S.C., WEED purchased S.C. tetrahydrocannabinol (THC) and emergency contraceptives the next morning and then drove S.C. back to her residence in Hyde Park. Law enforcement later canvassed the Crossroads Hotel and confirmed that WEED rented a room for two nights between March 25, 2022 and March 27, 2022 using a credit card. WEED's name and a phone number associated with WEED were included in the reservation record.

87. On June 13, 2022, NYSP facilitated a controlled phone call between S.C. (phone number [redacted]-3538) and WEED (phone number [redacted]2071). NYSP Investigators initiated the call from S.C.'s phone. WEED's phone number was saved in S.C.'s phone under the name "Mr. Salmon." Your affiant also confirmed that WEED provided the 2071 Number to S.C. over Snapchat on at least three occasions.

88. The topics discussed by WEED and S.C. during the controlled phone call corroborated many of the statements S.C. made during her initial interview with the NYSP. For example, S.C. asked WEED, "do you remember the videos at the hotel when we had sex." WEED

responded, "yeah." S.C. further asked WEED if he remembered when they were in the hotel, and he had to go get her "weed" to calm down. WEED replied, "yes" . . . "yeah, I remember that." WEED then asked, "how did they find everything?" S.C. responded that someone at her school had said something. WEED stated that they were careful not to show her face in the videos and further stated that the only way someone could have known it was S.C. is if that person knew what S.C. looked like "intimately." WEED further described the photos as "lingerie" photos and stated that such photos are not illegal. WEED suggested that they "don't do that business for a bit" and find other ways to make S.C. money.

89. Also, during the controlled call, WEED discussed several efforts he had made to conceal his "relationship" with S.C. For example, WEED mentioned changing his "Cash App name" and told S.C. he had deleted his "life" and had only recently reactivated Instagram because he thought "it might be fine." WEED also told S.C. that he unfriended S.C. on "Snap" just to be safe, but assured S.C. that if she needed him, he was there. WEED also referenced "the doc," which law enforcement later learned was a Google Doc WEED used to communicate with S.C. and take notes pertaining to their "relationship." During the call, WEED told S.C., "If you check the doc, I leave you goodnight and good morning messages." Thirty-two pages of this "doc" have since been seized by law enforcement. The text of the "doc" includes the parameters of WEED's "dominant/submissive" "relationship" with S.C., outlining rules that S.C. was expected to follow, as well as appropriate "rewards," "punishments," "boundaries," "routines," and "nicknames." The "doc" includes narratives and messages describing, in explicit detail, WEED's sexual fantasies involving S.C. The "doc" also contains the types of messages WEED mentioned during the controlled call. WEED also referenced the "Google Doc" or the "doc" multiple times during his

snapchat conversations with S.C. At least once during the controlled call, WEED stated that he needed to be cautious and asked S.C. if the call was being recorded.

90. On October 18, 2022, your affiant interviewed S.C. S.C. stated that within two hours of meeting WEED online, S.C. told WEED that she was 16 years old. WEED responded that they could just be friends, but within approximately a week, their conversations "turned sexual." S.C. also provided more detail regarding the sexually explicit nature of some of the photos and videos she exchanged with WEED primarily using Snapchat. For example, S.C. said that WEED elicited nude photos depicting her breasts and/or vagina. S.C. further stated that WEED asked for videos of her masturbating, using sex toys, and even asked her to record herself performing specific sex acts. S.C. admitted that some of the photos and videos she sent WEED were unsolicited. Furthermore, S.C. stated that WEED sent nude photos of himself to S.C., which depicted WEED's chest and/or penis.

91. During the October 18, 2022 interview, S.C. provided more detail regarding the arrangement she had with WEED regarding the sale of her explicit photos and videos. S.C. explained that WEED sold explicit images and videos that she sent to WEED via Snapchat. Using an Instagram account with the username "Jamesrweed1701," and possibly other means, WEED sold S.C.'s photos for $2 and her videos for $5. S.C. estimated that she received approximately $50-100 from the sale of her photos and videos. WEED also purchased items for her, such as clothing, coloring books, and colored pencils with the funds generated from S.C.'s photos and videos and as "rewards" within the context of their "Dominant/Submissive" "relationship." At one point, using Snapchat, WEED asked S.C. to login to the Instagram account using the e-mail [redacted]@gmail.com and the password "Jayman1701." According to S.C., she maintained

access to this Instagram account, but rarely logged in. S.C. was using an Android device to communicate with WEED during the relevant time period.

92. On October 18, 2022, after meeting with S.C., your affiant obtained consent from S.C., and her father to download S.C.'s Snapchat Data. As a result, your affiant was able to review, among other data, "Received/Sent Saved Chat History" between S.C.'s "babygirl_luna44" Snapchat account and other users, including "jayrw1701." In addition to S.C. confirming that "jayrw1701" was WEED's Snapchat account, the user of "jayrw1701" identified himself as "Jameson Weed" or "Jameson Ross Weed" at least a handful of times and provided personal identifying information, including the phone number listed in Paragraph 87 and WEED's address in Portsmouth, Virginia ("the Portsmouth Residence"). Moreover, the collective substance of the conversations that took place between the user of the "jayrw1701" account and S.C.'s "[redacted]4" account, combined with other information your affiant has gathered during the course of this investigation to-date, further suggests that WEED is in fact the user of the "jayrw1701" account."

93. Your affiant reviewed saved conversations between S.C. and WEED spanning from on or about January 28, 2022 through on or about June 12, 2022. The content of these conversations largely corroborated the statements S.C. made regarding the arrangement between her and WEED regarding the sale of her explicit photos and videos. It was clear from the substance of their conversation that WEED was managing the "Jamesrweed1701" Instagram account. WEED informed S.C. multiple times that her list of "followers" was growing. It was also evident that WEED and S.C. were collaborating on who to send photos and videos to, and to some degree, the content of those photos and videos. WEED also elicited photos and videos from S.C. on multiple occasions for himself through Snapchat. There was also a substantial amount of explicit content

exchanged between WEED and S.C. Moreover, your affiant also reviewed a substantial amount of content that appears consistent with efforts on WEED's behalf to "sexually groom" or develop an emotional connection with S.C in order to prepare S.C. to participate in sexual activity, specifically, sexual activity in connection with a dominant and submissive style "relationship" both in-person and virtually. The chats reviewed by your affiant also further corroborated the content of the controlled phone call described in Paragraphs 87-89.

94. During her October 2022 interview, S.C. further explained how she and WEED used Google Meet and Google Meet's chat feature to engage in virtual sexual encounters. This is also corroborated by the content of the consensual Snapchat download. Furthermore, within the chats, WEED provided two Gmail accounts on multiple occasions, including '[redacted]@gmail.com" and '[redacted]n@gmail.com." S.C. provided her Gmail account – '[redacted]@gmail.com."

95. On November 7, 2022, your affiant executed a Command Authorization Search and Seizure (CASS) Warrant at the Portsmouth Residence. Your affiant and other members of law enforcement located and seized two Android cellular devices from WEED's person and two additional Android cellular devices from WEED's bedroom. Forensic examination is still pending.

96. In my training and experience, evidence of who was using electronic accounts, such as the SUBJECT ACCOUNTS, and from where, and evidence related to criminal activity described herein, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

97. Based on my training and experience, stored data such as: instant messages, emails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to the SUBJECT ACCOUNTS may provide direct evidence of the offenses under investigation, and can also lead to the identification of co-conspirators, victims, and instrumentalities of the crimes under investigation.

98. In addition, the user's account activity, logs, stored electronic communications, and other data retained by the Providers can indicate who has used or controlled the SUBJECT ACCOUNTS. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time, and device identifiers and IP Addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

99. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

100. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional

identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

CONCLUSION

101. Based on the facts set forth above, I believe probable cause exists that Jameson Ross WEED has violated the TARGET OFFENSES.

102. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities (more precisely described in Attachments B-1, B-2, and B-3) of such violations will be found within the SUBJECT ACCOUNTS (more precisely described in Attachments A-1, A-2, and A-3).

103. Accordingly, I request that a warrant be issued authorizing your affiant, with assistance from additional NCIS agents and other law enforcement personnel, to search the SUBJECT ACCOUNTS described in Attachments A-1, A-2, and A-3 for the items specified in Attachments B-1, B-2, and B-3.

104. Because the warrant will be served on the Providers who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

FURTHER AFFIANT SAYETH NOT.

Stephen Barbour
NCIS Special Agent
Norfolk, VA

Subscribed and sworn before me on this 26th day of January, 2023, in the City of Norfolk, Virginia.

UNITED STATES MAGISTRATE JUDGE